INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

e-ISSN : 2583-1062

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 06, June 2024, pp: 2001-2005

Impact Factor: 5.725

SECURITY ISSUES AND RESEARCH CHALLENGES IN CLOUD COMPUTING

Mandeep Kaur Gulati[1]

[1]PG Deptt. of Computer Science Khalsa College for Women, Amritsar, India.

DOI: https://www.doi.org/10.58257/IJPREMS35193

ABSTRACT

Cloud Computing (CC) offers dynamically scalable services delivered over the Internet. The primary driver of cloud computing is its economic benefits, as it aims to reduce both capital and operational expenditures. Despite its advantages, there are still significant challenges that need to be addressed for widespread adoption. One of the critical issues is security and privacy concerns, which have been extensively researched but remain unresolved. Ensuring security is crucial for cloud adoption and the expansion of cloud deployment.This paper provides a detailed overview of the current cloud security challenges and mitigation strategies. It offers a comprehensive survey of underlying cloud security and privacy issues, along with the treats and risks, to better understand and address these persistent concerns.

Keywords: Cloud computing , Security, Cloud Security Issues, Threats, Vulnerabilities, Data protection

1. INTRODUCTION

In recent years, the demand for data has surged dramatically, and the number of online users has increased exponentially. Traditional computing infrastructure has become costly and challenging to manage, making it difficult to access data from anywhere at any time. As a result, external storage systems have become essential for data storage. Traditional computing can no longer handle the growing number of online users on networking sites, social media platforms, multimedia broadcasting, etc. With the global rise in internet usage, the increased volume and availability of services have led to the development of cloud computing.

Cloud computing offers numerous benefits, similar to other technological advancements. It enables the storage of large amounts of data and a variety of services. This platform addresses the problem of limited resources and reduces service costs by sharing valuable resources among multiple users. For reliable performance, the platform must be robust against security threats [1]. In recent years, cloud computing has become a significant focus in security research, covering areas such as data storage security, network security, and software security. The National Institute of Standards and Technology (NIST) defines cloud computing as [2] "a model for enabling convenient, resource pooling, ubiquitous, on-demand access which can be easily delivered with different types of service provider interaction."

Cloud computing follows a Pay as You Go (PAYG) model, where customers pay only for the services they use. This model allows customers to customize software, storage, development platforms, and computing resources according to their specific needs. These benefits have driven significant research efforts into this cutting-edge concept [3].

Cloud computing fundamentally provides three different service delivery models: Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). The SaaS model focuses on access management tasks in applications, such as policy controls, allowing multiple end users to benefit from a single instance of the service. Companies like Google, Microsoft Office 365, and Dropbox offer SaaS. In the PaaS model, a development environment layer is provided as a service, on which higher-level services can be built. Customers create their own applications running on the provider's infrastructure. PaaS offers a combination of OS and application servers like Microsoft Azure, Google App Engine, and LAMP platforms (Linux, Apache, MySQL, PHP), with a strong emphasis on data protection.

IaaS provides computing capabilities and essential storage as standardized services across the network. Virtualization is key in this model, arranging independent virtual machines (VMs) and isolating them from both the underlying hardware and other VMs. IaaS focuses on security areas such as firewalls, intrusion detection and prevention systems (IDS/IPS), and virtual machine monitors. Cloud computing is rapidly expanding, with more organizations adopting cloud technology daily. However, several security issues need attention. Examples of IaaS providers include Google Compute Engine (GCE), Amazon Web Services (AWS), Cisco Metapod, and Microsoft Azure.

Cloud computing encompasses various aspects, including cloud deployment models, which provide specific cloud environments distinguished by size, ownership, and accessibility. Cloud computing leverages resource sharing among individual devices or local servers. The purpose and nature of the cloud are associated with the deployment model, which includes three types: public cloud, private cloud, and hybrid cloud [4].

In the private cloud model, cloud computing deals with an organization's data center, with resources allocated to a single organization or multiple ones working inter-functionally. The infrastructure is owned and operated by the organization.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
www.ijprems.com
editor@ijprems.com
Vol. 04, Issue 06, June 2024, pp: 2001-2005
e-ISSN : 2583-1062
Impact Factor: 5.725

The public cloud model is owned and operated by governments, businesses, or academic institutions, providing open access over the internet or other portals. The hybrid cloud model combines private cloud resources with one or more external cloud services, with data and applications managed centrally. Each deployment model has specific advantages and disadvantages, with a shared responsibility security model underlying all cloud services. Both providers and consumers play a role in securing cloud-resident infrastructure and cloud-delivered applications.

The rest of the paper is organized as follows. Section 2 presents the literature review. In Section 3, cloud security issues and challenges are classifed and described. In Section 4, diferent security threats threatening cloud computing services are introduced. Finally, conclusions are presented in Section 5.

2. LITERATURE REVIEW

Cloud computing is an emerging paradigm that introduces numerous challenges, particularly in data security and access control [5]. Over the past decade, many survey papers have focused on the security challenges associated with cloud computing.

Sgandurra and Lupu [6] presented a taxonomy of attacks on virtualized systems, categorizing them based on their targets at different levels, the sources, and the goals of the attackers. Their work illustrates the evolution of threats, related security, and trust assumptions in virtualized systems across various layers such as hardware, operating systems, and applications.

Kaur and Singh [7] reviewed cloud computing security issues, discussing concerns related to data location, storage, security, availability, and integrity. While their review highlights significant security concerns, it is important to note that the authors focus solely on identifying issues without proposing possible solutions.

Kumar et al. [8] examined various data security issues in cloud computing and presented approaches to address these issues in a multi-tenant environment. Their paper is dedicated to data security issues and outlines methods for protecting data and ensuring its privacy.

Khalil et al. [9] conducted a review of cloud computing security and privacy concerns, classifying known security threats and attacks and identifying different cloud vulnerabilities. Their work also investigates the shortcomings of current solutions and discusses future security perspectives.

Bashir and Haider [10] provided a review of the most vulnerable security threats in cloud computing. This review considers both end users' and vendors' key security threats, offering analysis related to various security models and tools.

Ryan [11] conducted a survey identifying vital research directions, including methods for protecting data to ensure its safety from cloud infrastructure providers. This work also describes a browser key translation method that allows software-as-a-service applications to provide confidentiality services.

One of the long-envisioned goals of computing as a utility is cloud computing, which enables users to remotely store their data and access high-quality services from a shared pool of configurable computing resources [12]. As cloud technologies continue to progress, security risks become more sophisticated and new challenges emerge. Therefore, comprehensive research is needed to identify potential challenges and develop new solutions.

5. CLOUD SECURITY ISSUES AND CHALLENGES

Although cloud computing offers a range of beneficial services, it also presents numerous security threats and challenges. With a significant amount of information transferred over networks and stored in specific cloud resources, various vulnerabilities can be exploited by malicious actors. Various Cloud Computing issues and challenges are discussed below:

- **Access Controls:** Access control is a critical concern for all service providers, as inadequate controls can expose user data and allow hackers to infiltrate an organization's infrastructure [13] .
- **Accounting:** Accounting is a key aspect that must be measured when deploying services in cloud computing solutions to ensure proper network management [14] .
- **Compliance:** Cloud computing often struggles with supporting compliance management methods, which can lead to significant issues in data security and privacy [14] .
- **Cross-Organizational Security Management:** Achieving and maintaining security requirements and compliance with service level agreements (SLAs) is a major challenge in cloud computing. Effective security management requires collaboration among organizations to ensure that appropriate security measures are met [15] .
- **Extensibility and Shared Responsibilities:** Both service providers and users must prioritize security in cloud computing. Currently, there is no clear consensus on how security responsibilities should be distributed and managed in cloud environments [16] .

- **Private Cloud:** The concept of a private cloud involves on-premises infrastructure, akin to traditional computing environments. By utilizing virtualization technologies, computing resources can be dynamically scaled according to user needs. This allows for shared resource accessibility across entire departments within an organization. However, widespread implementation of private clouds has not yet been fully realized, making it a transitional step towards broader public cloud services [17].
- **Heterogeneity:** Heterogeneity issues arise when various service providers offer a wide range of services using different technologies. This can occur due to differences in software or hardware levels [18].
- **Identity Management (IdM):**Identity management is crucial in cloud computing security, aiming to perform verification and validation across diverse cloud services. However, it still faces challenges related to interoperability among the latest security technologies [19].
- **Integration:**When customers or organizations need to utilize multiple service providers for various reasons, they must integrate software and data across multiple clouds. This issue can sometimes be addressed by using hybrid clouds [17] .
- **Performance:** While cloud computing can reduce costs, performance issues such as communication delays between users and cloud services can become problematic. As the number of users grows, the volume of information and data transferred also increases, leading to high loads on hardware and software. Additionally, differences in distance between users and service providers can affect performance. Customers may also scale their cloud infrastructure beyond initial expectations, creating significant challenges for service providers [17].
- **Bandwidth Requirements:** Before implementing a cloud service, organizations must evaluate the communication bandwidth requirements and assess the services in terms of large data transmission volumes [17].
- **Monitoring:** Cloud computing necessitates extensive service monitoring, creating a substantial demand for monitoring activities across both public and private infrastructures [14].
- **Risk Analysis and Management:** Risk analysis and management are critical in cloud security. This involves reducing the load capacity in cloud computing by identifying and scanning for risks before providing services to customers [14].
- **Service Level Agreements (SLAs):** SLAs are vital components of the contractual relationship between cloud service customers and providers. Given the global nature of the cloud, SLAs often span multiple jurisdictions with varying legal requirements, particularly concerning the protection of personal data hosted in the cloud [20].
- **Virtualization:** Virtualization is a key method for delivering cloud services, especially IaaS, but it still encounters security issues [18] .
- **Policies:** Cloud computing requires well-crafted policies for security procedures and guidelines to be implemented effectively [21].
- **Security in Web Browsers:** The security capabilities of web browsers are often insufficient for handling user needs in complex and sophisticated environments, such as banking and critical applications, within shared cloud solutions [22].

6. CLOUD COMPUTING THREATS AND RISKS

Many recent studies have identified various threats, including data breaches, hacked interfaces and application programming interfaces (APIs), exploited system vulnerabilities, account hijacking, malicious insiders, and denial-of-service (DoS) attacks etc. These threats and attacks are discussed below:

- **Data Breaches:** Data breaches are a significant concern for cloud customers, involving the unauthorized release, viewing, theft, or use of protected or confidential information such as credit card numbers or Social Security numbers
- **Account and service hijacking:** Account and service hijacking is a critical security threat where attackers compromise a web service hosted on a cloud server or service provider. They then install malicious control software within the cloud provider's infrastructure, gaining unauthorized control and access [23].
- **Abuse and Nefarious Use of Cloud Computing:** In this type of threat, attackers exploit the computing power of cloud infrastructure to launch attacks on targets using spam and malware, such as botnets. According to the Cloud Security Alliance (CSA), this is one of the top security threats in cloud computing [24] .
- **Backdoor Channel Attacks:**These attacks occur in Infrastructure-as-a-Service (IaaS) environments when users are granted high permissions on virtual machines (VMs) or at the hypervisor level. This can compromise service availability and data privacy [25].
- **Cross-Site Scripting (XSS) Attacks :** XSS attacks exploit security weaknesses in web applications. One of the most commonly used scripting languages for these attacks is JavaScript [26].

- **Cloud Malware Injection Attacks:** Among the top cloud computing security threats, this attack involves injecting malicious software, applications, or virtual machines into the cloud infrastructure [27] .
- **Denial of Service (DoS) Attacks:** In a DoS attack, services become unavailable to users attempting to access them, often resulting in an error 404 indicating that the service is not found [26] .
- **Insecure Application Programming Interfaces (APIs):** This issue arises when service providers deliver services to customers using APIs that lack proper encryption, secure authentication, access control, and activity monitoring mechanisms [28].
- **Man-in-the-Middle Attacks:** In these attacks, a hacker intercepts communication between a customer and a service provider, covertly observing data and information without the knowledge of either party [26].
- **Metadata Spoofing Attacks:** In this attack, web service providers send a metadata document to the client's system containing information about service invocation, such as security requirements, message format, and network location. The attacker aims to reengineer these metadata descriptions to alter network references and endpoints to the security policies [29].
- **Malicious Insiders:** This threat occurs when there is insufficient security to control how employees access virtual properties of the cloud. The threat becomes more complex due to employees' privileges and the lack of updated responsibilities when their roles or behavior change [23].
- **Phishing Attacks:** Phishing attacks compromise user privacy and data by tricking users into accessing fake web links installed on their PCs, where malicious codes then expose the data [23].
- **SQL Injection Attacks:** These attacks target website databases by injecting malicious SQL statements through website inquiry methods, potentially disabling website security [26].
- **Shared Technology Vulnerabilities:** This issue arises from cloud computing using the same infrastructures as the internet, shared among cloud customers. Consequently, existing internet infrastructure problems migrate to the cloud, as traditional components were not developed for resource sharing in cloud computing systems [23].
- **Sniffer Attacks:** In sniffer attacks, the attacker aims to read the content of network packets, particularly when no encryption methods are applied during data transmission. A sniffer can be a script, application, or device [26].
- **Security Concerns with Virtual Machine Managers:**This security issue arises from the need for service providers to be extremely vigilant when offering services through VM technology, as it can have various security vulnerabilities in certain cases [26] .
- **Unknown Risk Profiles:**This type of security threat emerges from focusing on the functionalities and features gained from implementing cloud services without adequately considering the security technologies and protocols to be developed. The concern is that features may allow third-party access to data, which could be disclosed for various reasons [23].
- **Zombie Attacks (DoS/DDoS):**These attacks involve indirect or direct flooding at the Hypervisor, Network, or VM level, affecting service availability and potentially creating user accounts for unauthorized service usage [23].

7. CONCLUSION

The rapid adoption of cloud computing has revolutionized the way organizations manage and store data, offering substantial benefits such as simplified IT infrastructure, remote accessibility, and cost efficiencies. However, these advantages come with significant security and privacy challenges that require thorough examination and effective solutions. This survey has provided a comprehensive review of the security issues and requirements in cloud computing, highlighting identified threats and known vulnerabilities. Additionally, various security threats have been discussed that pose risks to cloud computing services, emphasizing the need for ongoing vigilance and innovation in security practices. In conclusion, the security challenges faced by cloud entities such as cloud service providers, data owners, and cloud users are complex and multifaceted. Addressing these challenges necessitates a collaborative approach involving academia, industry, and standards organizations. As cloud computing continues to evolve, it is imperative to develop robust security strategies that can protect against emerging threats and ensure the privacy and integrity of data in the cloud.

8. REFERENCES

[1] Subramanian N, Jeyaraj A (2018) Recent security challenges in cloud computing. Comput Electr Eng 71:28–42
[2] Mell P, Grance T (2018) SP 800-145, The NIST Defnition of cloud computing | CSRC (online) Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-145/fnal. Accessed 11 Dec 2018
[3] Xu X (2012) From cloud computing to cloud manufacturing. Robot Comput Integr Manuf 28(1):75–86
[4] Bhamare D, Samaka M, Erbad A, Jain R, Gupta L, Chan HA (2017) Optimal virtual network function placement in multi-cloud service function chaining architecture. Comput Commun 102:1–16

[5] Yu S, Wang C, Ren K, Lou W (Mar 2010) Achieving secure, scalable, and fne-grained Data access control in cloud computing. In: Proceedings of the IEEE INFOCOM

[6] Sgandurra D, Lupu E (2016) Evolution of attacks, threat models, and solutions for virtualized systems. ACM Comput Surv 48(3):1–38

[7] Kaur M, Singh H (2015) A review of cloud computing security issues. Int J Adv Eng Technol 8(3):397–403

[8] Kumar PR, Raj PH, Jelciana P (2018) Exploring data security issues and solutions in cloud computing. Proc Comput Sci 125:691–697

[9] Khalil I, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35

[10] Bashir SF, Haider S (Dec 2011) Security threats in cloud computing. In: Proceedings of the International Conference for Internet Technology and Secured Transactions, pp 214– 219.

[11] Ryan MD (2013) Cloud computing security: the scientifc challenge, and a survey of solutions. J Syst Softw 86(9): 2263–2268.

[12] Wang C, Wang Q, Ren K, Lou W (Mar 2010) Privacy-preserving public auditing for data storage security in cloud computing. In: Proceedings of the IEEE INFOCOM

[13] Zissis, D. and D. Lekkas (2012) Addressing cloud computing security issues. Future Generation computer systems, 28(3) 583-592.

[14] Moreno-Vozmediano, R., R.S. Montero, and I.M. Llorente (2013) Key challenges in Cloud computing: Enabling the future internet of services. Internet Computing, IEEE, 17(4) 18-25.

[15] Khalil, I.M., A. Khreishah, and M. Azeem (2014) Cloud computing security: a survey. Computers, 3(1) 1-35.

[16] Zhang, L., et al., (2014) Cloud manufacturing: a new manufacturing paradigm. Enterprise Information Systems, 8(2), 167-187.

[17] Kim, W., et al. (2009) Adoption issues for cloud computing. in Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia. ACM.

[18] Crago, S., et al. (2011) Heterogeneous cloud computing. in Cluster Computing (CLUSTER), 2011 IEEE International Conference on. IEEE.

[19] Lar, S.-U., X. Liao, and S.A. Abbas (2011) Cloud computing privacy & security global issues, challenges, & mechanisms. in Communications and Networking in China (CHINACOM), 2011 6th International ICST Conference on. IEEE.

[20] Oliveira, A.C., et al. (2014) Efficient network service level agreement monitoring for cloud computing systems. in Computers and Communication (ISCC), IEEE Symposium on. (2014). IEEE

[21] Zhang, Q., L. Cheng, and R. Boutaba (2010) Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1) 7-18.

[22] Wei, L., et al., (2014) Security and privacy for storage and computation in cloud computing. Information Sciences, 258 371-386.

[23] Younis, M. and K. Kifayat (2013) Secure cloud computing for critical infrastructure: A survey. Liverpool John Moores University, United Kingdom, Tech. Rep

[24] Khorshed, M.T., A.S. Ali, and S.A. Wasimi (2012) A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation computer systems, 28(6) 833-851.

[25] Modi, C., et al., (2013) A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications, 36(1) 42-57.

[26] Subbiah, M., Muthukumaran D.S.S., and Ramkumar D. (2013) Enhanced Survey and Proposal to secure the data in Cloud Computing Environment. International Journal of Engineering Science, 5.

[27] Chou, T.-S. (2013) Security threats on cloud computing vulnerabilities. International Journal of Computer Science & Information Technology, 5(3) 79.

[28] Akande, A.O., N.A. April, and J.-P. Van Belle (2013) Management Issues with Cloud Computing. in Proceedings of the Second International Conference on Innovative Computing and Cloud Computing. ACM.

[29] Jensen, M., N. Gruschka, and R. Herkenhöner (2009) A survey of attacks on web services. Computer Science-Research and Development, 24(4) 185-197.